UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,983	03/31/2004	Hashem Mohammad Ebrahimi	1565.069US1	9751

21186 7590 07/08/2009

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
07/08/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@slwip.com

Office Action Summary	Application No.	Applicant(s)	
	10/814,983	EBRAHIMI ET AL.	
	Examiner	Art Unit	
	Thomas Gyorfi	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-15,17-22 and 24-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-15,17-22 and 24-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/21/09*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 2, 4-15, 17-22, and 24-26 remain for examination. The correspondence filed 4/21/09 amended claims 1, 8, 15, 21, and 25.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/21/09 has been entered.

Response to Arguments

3. Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection. However, in response to Applicant's traversal of Official Notice, Examiner wishes to remind Applicant once again for the record that Examiner had already provided multiple references establishing the obviousness of the disputed limitations: U.S. Patent 7,430,757 to Chari and U.S. Patent 6,732,269 to Baskey (see the Final Office Action of 1/21/09, page 4, last paragraph; cf. pages 6, 8, & 10). Applicant had ample time in which to consider the teachings of these references, and in particular observe that Chari in particular discloses the new limitations in full as shall be discussed below.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1, 2, 4-15, 17-22, and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over "The Netscape Proxy Server Version 3.5 for Unix Administrator's Guide" (hereinafter, "Netscape") in view of Green et al. (U.S. Patent 6,003,084) in view of Chari et al. (U.S. Patent 7,430,757).

Regarding claim 1:

Netscape discloses a method comprising: receiving a secure communication request from a client (Chapter 14, page 2, Figure 14.1 and 1st paragraph); identifying a domain identification associated with the request (inherent to proxying in general; cf. Chapter 6, e.g. "Enabling Proxying for a Resource"); and routing the request to a proxy based on the domain identification, wherein the proxy communicates securely with the external domain via a first set of unique session keys used for the local domain accelerator and the external domain (Chapter 14, "Setting up Client Authentication in a Reverse Proxy", cf. "Content Server Authenticates Proxy") and separately the local domain accelerator communicates securely with the client via a second set of unique session keys used for the local domain accelerator and the client to communicate (Chapter 14, "Setting up Client Authentication in a Reverse Proxy", cf. "Proxy Authenticates Client") and the first set of session keys and the second set of session keys are different from one another (Ibid, by virtue of being inherent to the multiple SSL

connections disclosed) and wherein the client believes communication that the client has with the local domain accelerator is occurring with the external domain but in fact it occurs with the local domain accelerator via the second set of session keys ("What Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 7, "How Reverse Proxying Works"), and wherein the local domain accelerator caches data from the external domain for servicing the request of the client and maintained in decrypted format within the cache (see all of Chapter 9, beginning with "How Caching Works").

Netscape appears to be silent regarding wherein the local domain accelerator vends an external domain certificate to the client during the communication to present itself as the external domain. However, Green discloses an analogous proxy server wherein the proxy stores the server's authentication certificate and vends it to the client during the negotiation phase between the client and the proxy (col. 10, lines 7-47; see also col. 9, lines 25-35).[1] It would have been obvious to modify the Netscape proxy server to use the external domain's certificate in negotiating the SSL connection between itself and the client in order to represent itself as the server to the client, because the technique was clearly a known improvement that was well within the capabilities of one of ordinary skill in the art, in view of the teaching of the technique in an equivalent proxy server. Green further discloses that this technique is advantageous because it provides security to an otherwise insecure connection without requiring any modification to either the client or the server (col. 6, lines 15-20; col. 9, lines 1-10).

[1] Examiner reminds the Applicant that SSL encryption, such as that employed by Netscape, typically uses X.509 certificates for authentication in much the same manner as disclosed by Green (see the "Secure Sockets Layer Protocol (SSL)" reference from the Office Action of 2/1/08, page 3, "SSL Supported Methods").

With regards to the new limitations regarding encrypted communications for both links, although the Examiner stands by his previous assertion that the Netscape reference discloses multiple encrypted connections, even were that not the case then Examiner observes that Chari discloses an SSL proxy between a client and a server wherein communications from one to the other are encrypted using a first session key, sent to the proxy, decrypted by said proxy, and re-encrypted using the second session key (col. 8, lines 1-30). The claim is thus obvious because the ability to have a proxy maintain separate session keys/secure connections between itself and each of a client and server was clearly within the capabilities of one of ordinary skill in the art.

Regarding claim 8:

Netscape discloses a method comprising: receiving a secure request forwarded from a proxy, the secure request originating from a client and destined for an external domain (Chapter 14, page 2, Figure 14.1 and 1st paragraph); establishing a secure communication with the client by providing the client a certificate associated with an external domain (Chapter 5, "Controlling Access with Client Certificates") and wherein the secure communication entails using a first set of session keys to communicate securely with the client and the client believes after receiving the certificate that communication is occurring with the external domain (Chapter 14, "Setting up Client Authentication in a Reverse Proxy", cf. "Proxy Authenticates Client"; Chapter 7, "How Reverse Proxying Works"); and servicing the client with data that is acquired from the external domain, and wherein a portion of that data is used to service the request (all of

Chapter 9), and wherein separate communication is securely established with the external domain using a second set of session keys different from the first set of session keys (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Content Server Authenticates Proxy”) and wherein the data is maintained in decrypted format within the cache (Chapter 9, Ibid).

Netscape appears to be silent regarding wherein the local domain accelerator vends an external domain certificate to the client during the communication to present itself as the external domain. However, Green discloses an analogous proxy server wherein the proxy stores the server's authentication certificate and vends it to the client during the negotiation phase between the client and the proxy (col. 10, lines 7-47; see also col. 9, lines 25-35). It would have been obvious to modify the Netscape proxy server to use the external domain's certificate in negotiating the SSL connection between itself and the client in order to represent itself as the server to the client, because the technique was clearly a known improvement that was well within the capabilities of one of ordinary skill in the art, in view of the teaching of the technique in an equivalent proxy server. Green further discloses that this technique is advantageous because it provides security to an otherwise insecure connection without requiring any modification to either the client or the server (col. 6, lines 15-20; col. 9, lines 1-10).

With regards to the new limitations regarding encrypted communications for both links, although the Examiner stands by his previous assertion that the Netscape reference discloses multiple encrypted connections, nevertheless Examiner observes that Chari discloses an SSL proxy between a client and a server wherein

communications from one to the other are encrypted using a first session key, sent to the proxy, decrypted by said proxy, and re-encrypted using the second session key (col. 8, lines 1-30). The claim is thus obvious because the ability to have a proxy maintain separate session keys/secure connections between itself and each of a client and server was clearly within the capabilities of one of ordinary skill in the art.

Regarding claim 15:

Netscape discloses a system comprising: a proxy (e.g. “What Netscape Proxy Server Provides”); and a local domain accelerator implemented in a computer-readable medium and to process on the proxy (Ibid, but particularly the 3rd and 4th paragraphs; cf. Chapter 9, “How Caching Works”) wherein a client securely requests an external domain and the proxy routes the request to the local domain accelerator [i.e. itself], the local domain accelerator securely communicates with the external domain and services the client via encrypted communications (Chapter 14, e.g. "Tunneling SSL through the Proxy Server"), and caches data in a local cache of the proxy in a decrypted format which is used to service the client via secure communications between the local domain accelerator and the client (Chapter 9, "How Caching Works") and wherein the proxy communicates securely with the external domain via a first set of unique session keys used for the local domain accelerator and the external domain (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Content Server Authenticates Proxy”) and separately the local domain accelerator communicates securely with the client via a second set of unique session keys used for the local domain accelerator and the client

to communicate (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Proxy Authenticates Client”) and the first set of session keys and the second set of session keys are different from one another (Ibid, by virtue of being inherent to the multiple SSL connections disclosed) and wherein the client believes communication that the client has with the local domain accelerator is occurring with the external domain but in fact it occurs with the local domain accelerator via the second set of session keys ("What Netscape Proxy Server Provides”, 2nd and 5th paragraphs; Chapter 7, “How Reverse Proxying Works”).

Netscape appears to be silent regarding wherein the local domain accelerator vends an external domain certificate to the client during the communication to present itself as the external domain. However, Green discloses an analogous proxy server wherein the proxy stores the server's authentication certificate and vends it to the client during the negotiation phase between the client and the proxy (col. 10, lines 7-47; see also col. 9, lines 25-35). It would have been obvious to modify the Netscape proxy server to use the external domain's certificate in negotiating the SSL connection between itself and the client in order to represent itself as the server to the client, because the technique was clearly a known improvement that was well within the capabilities of one of ordinary skill in the art, in view of the teaching of the technique in an equivalent proxy server. Green further discloses that this technique is advantageous because it provides security to an otherwise insecure connection without requiring any modification to either the client or the server (col. 6, lines 15-20; col. 9, lines 1-10).

With regards to the new limitations regarding encrypted communications for both links, although the Examiner stands by his previous assertion that the Netscape reference discloses multiple encrypted connections, nevertheless Examiner observes that Chari discloses an SSL proxy between a client and a server wherein communications from one to the other are encrypted using a first session key, sent to the proxy, decrypted by said proxy, and re-encrypted using the second session key (col. 8, lines 1-30). The claim is thus obvious because the ability to have a proxy maintain separate session keys/secure connections between itself and each of a client and server was clearly within the capabilities of one of ordinary skill in the art.

Regarding claim 21:

Netscape discloses a system comprising: a local domain accelerator implemented in a computer-readable medium and to process on a proxy (“What Netscape Proxy Server Provides”, 3rd and 4th paragraphs; Chapter 9, "How Caching Works"); and cache of the proxy (Ibid) wherein the local domain accelerator securely communicates with a client as if the local domain accelerator was an external domain [i.e. a proxy] and securely communicates with the external domain for purposes of acquiring data from the external domain (Chapter 14, e.g. "Tunneling SSL through the Proxy Server"), wherein the proxy communicates securely with the external domain via a first set of unique session keys used for the local domain accelerator and the external domain (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Content Server Authenticates Proxy”) and separately the local domain accelerator

communicates securely with the client via a second set of unique session keys used for the local domain accelerator and the client to communicate (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Proxy Authenticates Client”) and the first set of session keys and the second set of session keys are different from one another (Ibid, by virtue of being inherent to the multiple SSL connections disclosed) and wherein the client believes communication that the client has with the local domain accelerator is occurring with the external domain but in fact it occurs with the local domain accelerator via the second set of session keys ("What Netscape Proxy Server Provides”, 2nd and 5th paragraphs; Chapter 7, “How Reverse Proxying Works”).

Netscape appears to be silent regarding wherein the local domain accelerator vends an external domain certificate to the client during the communication to present itself as the external domain. However, Green discloses an analogous proxy server wherein the proxy stores the server's authentication certificate and vends it to the client during the negotiation phase between the client and the proxy (col. 10, lines 7-47; see also col. 9, lines 25-35). It would have been obvious to modify the Netscape proxy server to use the external domain's certificate in negotiating the SSL connection between itself and the client in order to represent itself as the server to the client, because the technique was clearly a known improvement that was well within the capabilities of one of ordinary skill in the art, in view of the teaching of the technique in an equivalent proxy server. Green further discloses that this technique is advantageous because it provides security to an otherwise insecure connection without requiring any modification to either the client or the server (col. 6, lines 15-20; col. 9, lines 1-10).

With regards to the new limitations regarding encrypted communications for both links, although the Examiner stands by his previous assertion that the Netscape reference discloses multiple encrypted connections, nevertheless Examiner observes that Chari discloses an SSL proxy between a client and a server wherein communications from one to the other are encrypted using a first session key, sent to the proxy, decrypted by said proxy, and re-encrypted using the second session key (col. 8, lines 1-30). The claim is thus obvious because the ability to have a proxy maintain separate session keys/secure connections between itself and each of a client and server was clearly within the capabilities of one of ordinary skill in the art.

Regarding claims 2 and 19:

Netscape further discloses one of a forward proxy and a transparent proxy ("What Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 14, "Using Encryption in the Proxy Server, 2nd paragraph).

Regarding claims 4 and 18:

Netscape further discloses establishing a Secure Sockets Layer (SSL) handshake between the client and the local domain accelerator to service the request, wherein the client believes that the handshake is with external domain (Chapter 14).

Regarding claim 5:

Netscape further discloses intercepting the request that originates from the client to the external domain (inherent to proxies by definition; see also Chapter 6, “Sending the Client's IP Address to the Server”, wherein by default the proxy intercepts a client request to replace the client's IP address with the proxy’s IP address).

Regarding claims 6 and 10:

Netscape further discloses accessing, by the local domain accelerator, caching services for caching and managing the data (all of Chapter 9).

Regarding claim 7:

Netscape further discloses wherein stripping a host header from the request, host header being the domain identifier that identifies the external domain (inherent to proxies by definition; see also Chapter 5, “Allowing Access to a Resource”).

Regarding claim 9:

Netscape further discloses acting as the external domain when interacting with the client (inherent to being a transparent proxy: "What Netscape Proxy Server Provides”, 2nd and 5th paragraphs; Chapter 14, "Using Encryption in the Proxy Server, 2nd paragraph).

Regarding claim 11:

Netscape further discloses acquiring at least a portion of the data from the external domain in advance of a subsequent request for that portion of the data, wherein the subsequent request is issued from the client (Chapter 9, “Using Cache Batch Updates").

Regarding claim 12:

Netscape further discloses interacting securely with the external domain to acquire the data housed in the local cache (Ibid; secure connections disclosed in Chapter 14, e.g. “Setting Up Client Authentication in a Reverse Proxy").

Regarding claims 13 and 17:

Netscape further discloses wherein interacting securely further includes mutually signing interactions transmitted between the local domain accelerator and the external domain, as this is inherent to SSL (“The Secure Socket Layer Protocol (SSL)”, page 3, “SSL – Authentication and Integrity”; cf. Netscape, Chapter 5, “Controlling Access with Client Certificates”; see also RFC2246, e.g. page 41).

Regarding claim 14:

Netscape further discloses using the proxy to establish a secure communications channel between the local domain accelerator and the external domain (Chapter 14, e.g. Figure 14.2 and “Setting Encryption Preferences”).

Regarding claims 20 and 22:

Netscape further discloses wherein the proxy creates a secure communications tunnel between the client and the local domain accelerator and the proxy creates a secure communications channel between the local domain accelerator and the external domain (Chapter 7, "Setting Up a Secure Reverse Proxy"; Chapter 14, "Setting up Client Authentication in a Reverse Proxy").

Regarding claim 24:

SSL as implemented by Netscape inherently requires an exchange of certificates during communications between two parties (see "The Secure Sockets Layer Protocol (SSL)", page 3, "SSL – Authentication and Integrity"; cf. Netscape, Chapter 5, "Controlling Access with Client Certificates"; see also RFC2246, page 23).

Regarding claim 25:

Netscape further discloses wherein the client is a browser using SSL (e.g. Netscape Navigator: "What Netscape Proxy Server Provides", 6th paragraph; Chapter 14, "What is HTTPS?"), and the local domain accelerator intercepts and forwards communications toward a proxy and the proxy forwards communications to the local domain accelerator where the local domain accelerator presents itself securely to the client as if it were the external domain (Chapter 6, "Mapping URLs to Other URLs"; Chapter 7, "How Reverse Proxying Works" and "Setting Up a Secure Reverse Proxy").

Regarding claim 26:

Netscape further discloses a plurality of external sites featuring a plurality of services (e.g. Chapter 7, "Proxying for Load Balancing").

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
6/22/09

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435